Cryptology ePrint Archive: Report 2011/052

Revocable Attribute-Based Signatures with Adaptive Security in the Standard Model

Alex Escala and Javier Herranz and Paz Morillo

Abstract: An attribute-based signature with respect to a signing policy, chosen ad-hoc by the signer, convinces the verifier that the signer holds a subset of attributes satisfying that signing policy. Ideally, the verifier must obtain no other information about the identity of the signer or the attributes he holds. This primitive has many applications in real scenarios requiring both authentication and anonymity/privacy properties.

We propose in this paper the first attribute-based signature scheme satisfying at the same time the following properties: (1) it admits general signing policies, (2) it is proved secure against fully adaptive adversaries, in the standard model, and (3) the number of elements in a signature depends only on the size of the signing policy. Furthermore, our scheme enjoys the additional property of revocability: an external judge can break the anonymity of a signature, when necessary. This property may be very interesting in real applications where authorities are unwilling to allow full anonymity of users.

Category / Keywords: cryptographic protocols / attribute-based signatures, Groth-Sahai proofs, unforgeability, non-linkability, revocability

Date: received 27 Jan 2011

Contact author: jherranz at ma4 upc edu